NSv 270/470/870

SonicWallネットワークセキュリティバーチャルNSv 270/470/870ファイアウォールは、エンタープライズクラスのセキュリティ、管理の合理化、高い可視性、導入における柔軟性に加え、バーチャルワークロードに対して卓越したパフォーマンスを提供します。

セキュリティへ影響や課題をもたらす仮想環境における脆弱性が、新たに見つかりつつあります。一部のセキュリティ障害は効果的ではないポリシーや誤った構成によるものであるため、これらのすべてのセキュリティ経路を防御するには、一貫性のある適切なセキュリティポリシーを適切なネットワーク制御ポイントに適用できる機能も必要です。

ハイライト

パブリッククラウド、プライベートクラウド、ガバメントクラウドのセキュリティ

- 自動化リアルタイムの侵入検知および防止機能をもつ次世代ファイアウォール
- 特許取得済みのReal-Time Deep Memory Inspection（RTDMI™）テクノロジー
- 特許取得済みのReassembly-Free Deep Packet Inspection（RFDPI）テクノロジー
- 統合ポリシーによる完全にエンドツーエンドの可視性と管理の合理化
- アプリケーションのインテリジェンスと制御
- DNSセキュリティ
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）
- Wi-Fi 6ファイアウォールの管理
- Aruba ClearPassによるネットワークアクセス制御の統合
- AWSおよびAzure米国政府向けクラウドのサポート
- Microsoft Azure Sentinelとの統合による迅速なインシデント対応
- プライベートクラウド（ESXi、Hyper-V、KVM、Nutanix）およびパブリッククラウド（AWS、Azure）プラットフォームのサポート

仮想マシンの保護

- データの機密性
- データ漏洩防止による安全な通信
- トラフィックの検証、インスペクションおよびモニタリング
- 仮想ネットワークの回復性と可用性

データシート

NSvファイアウォールシリーズは、業務上重要なサービスや活動に深刻な影響を与えるセキュリティ上のリスクや脆弱性を抑制することにより、セキュリティチームを支援します。このため、企業はファイアウォールを通過する動的なトラフィックを制御して、異なるポリシーに対する可視性とインサイトを提供できます。その結果、管理タスクの簡素化、構成におけるエラーの減少、導入に要する時間の短縮が可能になり、全社的なセキュリティ体制の向上に貢献します。

SonicOSXとセキュリティサービス

NSv 270/470/870ファイアウォールの中心はSonicOSXアーキテクチャです。本シリーズは、SonicOSX 7オペレーティングシステムを搭載し、直感的なユーザーインターフェイス(UI)、高度なセキュリティ、ネットワーキング、管理機能などを豊富に備えています。

SonicOSX 7.0はゼロから構築されており、統合ポリシーの機能によってさまざまなセキュリティポリシーを総合的に管理します。レイヤー3からレイヤー7までの制御をすべてのファイアウォール上の1つのルールベースで簡単にプロビジョニングでき、ポリシーの構成を一元的に行えます。新しいWebインターフェイスにより、重要な脅威の情報を視覚化します。また、アラートを表示して簡単なポイント&クリック動作でコンテキストに応じたセキュリティポリシーを設定するように促します。

NSvでは、SD-WAN、TLS 1.3サポート、リアルタイム表示、高速VPN(Virtual Private Network)など、強固なセキュリティ機能も統合しています。未知の脅威は、SonicWallのクラウドベースのマルチエンジンサンドボックスであるCapture ATP(Advanced Threat Protection)に送信され、分析されます。Capture ATPは、SonicWallの特許取得済みテクノロジーであるReal-Time Deep Memory Inspection(RTDMI)を活用してメモリ内のマルウェアやゼロデイ攻撃の脅威を発見し、ブロックします。

Capture ATP、RTDMIテクノロジー、高度なセキュリティサービスの組み合わせによって、NSvシリーズのファイアウォールは、マルウェアが重要なシステムに到達する前にゲートウェイで阻止します。

導入

1. クラウド境界:パブリッククラウド、プライベートクラウド、ガバメントクラウドの保護

- Amazon Web Services(AWS)およびMicrosoft Azureでのワークロードの保護
- VPN、IPS、CFS、AVなどの機能を備えた高度な次世代ファイアウォール機能でクラウドアプリケーションとクラウドインフラストラクチャをサイバー脅威から保護
- 暗号化されたトラフィックを簡単に復号でき、TLS 1.3サポートを利用してセキュリティを強化
- 脅威防御とセグメンテーション機能の実装により規制基準の順守を確保
- 統合ポリシーによる、複数リージョンとアベイラビリティーゾーン全体にわたるトラフィックの完全な可視化と制御
- CAPEX(設備投資)からOPEX(営業経費)への移行による費用便益と効率性の実現
- NSvファイアウォールの導入による、米国政府機関とその顧客向けAWSおよびAzureクラウドの保護
- 仮想化されたコンピューティングリソースとハイパーバイザを保護し、VMware ESXi、Microsoft Hyper-V、Nutanix、KVM上のプライベートクラウドワークロードを防御
- 仮想マシン間のホスト内通信を完全に可視化して脅威から防御
- 仮想環境全体へのセキュリティポリシーの適切な適用
- VMの場所を問わず、アプリケーション、ユーザー、デバイスごとに安全なアプリケーション有効化ルールを提供
- 適切なセキュリティゾーニングと分離の実装
- Microsoft Azure Sentinelとの統合による、拡張性、クラウドネイティブ、セキュリティ情報イベント管理(SIEM)、インシデント対応を強化するセキュリティオーケストレーション自動対応(SOAR)ソリューション

2. インターネット境界

- インターネットゲートウェイで攻撃から企業リソースを防御
- 高度なセキュリティ機能でインターネット境界を高度な攻撃から保護し、脅威を自動的にブロック
- 脅威防御とセグメンテーション機能の実装により規制基準の順守を確保
- SonicOSXの機能強化を活用し、ビジネスの効率と業績の改善およびコスト削減を実現
- クリティカルなPoS(Point of Sale)システムをセグメント化し、事業継続性を確保
- 統合ポリシーによる、複数リージョンとアベイラビリティーゾーン全体にわたるトラフィックの完全な可視化と制御

NSvシリーズのシステム仕様

ファイアウォールの概要	NSv 270	NSv 470	NSv 870
オペレーティングシステム	SonicOSX[11]		
サポートされるハイパーバイザ	VMware ESXi v5.5/v6.0/v6.5/v6.7/v7.0/v8.0、Microsoft Hyper-V、KVM Ubuntu 16.04 / CentOS 7、Nutanix AHV（AOS 5.15 LTS/Prism Central 5.16.1.2）[10]		
ガバメントクラウドのサポート[12]	AWSおよびAzure（米国東部および西部地域）		
AWSインスタンスタイプのサポート	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
Azureインスタンスタイプのサポート	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
ライセンス	BYOL、PAYG[1]		
サポートされる最大vCPU	2	4	8
インターフェース数（ESXi/Hyper-V/KVM/Nutanix/AWS/Azure）	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
管理プレーン/データプレーンの最大コア数	1/1	1/3	1/7
必要最低メモリ[2]	4GB	8GB	10GB
最大メモリ[3]	6GB	10GB	14GB
サポートされるIP数/ノード	無制限		
必要最低ストレージ	60GB		
SSOユーザー数	500	10,000	15,000
ログ機能	アナライザー、ローカルログ、Syslog		
高可用性	アクティブ/パッシブ[4]		

ファイアウォール/VPNパフォーマンス[5,7]	NSv 270	NSv 470	NSv 870
ファイアウォールインスペクションのスループット	6 Gbps	9 Gbps	14 Gbps
脅威防御のスループット	1.6 Gbps	2.9 Gbps	8 Gbps
IPSスループット	4 Gbps	6 Gbps	8 Gbps
TLS/SSL DPIスループット	800 Mbps	2 Gbps	4 Gbps
VPNのスループット[8]	1.4 Gbps	3.5 Gbps	8 Gbps
接続数/秒	13,760	37,270	75,640
最大接続数 (SPI)	225,000	1.5M	3M
最大接続数 (DPI)	125,000	1.5M	2M
TLS/SSL DPI接続数	8,000	20,000	30,000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
サイト間VPNトンネル数	75	6,000	10,000
IPSec VPNクライアント[13] (最大)	50(1,000)	2,000(4,000)	2,000(6,000)
SSL VPNクライアントを含む[6]	2	2	2
SSL VPNクライアント(最大)[6]	100	200	300
暗号化/認証	DES、3DES、AES(128、192、256-ビット)/MD5、SHA-1、Suite B、Common Access Card (CAC)		
キー交換	Diffie Hellmanグループ1、2、5、14v		
ルートベースVPN	スタティックRIP、OSPF、BGP		
ネットワーク	**NSv 270**	**NSv 470**	**NSv 870**
IPアドレスの割り当て	スタティック、DHCP、内部DHCPサーバー[9]、DHCPリレー[9]		
NATモード	1対1、多対1、1対多、フレキシブルNAT(複IP)、PAT		
論理VLANおよびトンネルインターフェイス(最大)[7]	128	128	128
ルーティングプロトコル	BGP、OSPF、RIPv1/v2、スタティックルート、ポリシーベースのルーティング		
QoS	帯域幅の優先度、最大帯域幅、保証帯域幅、DSCPマーキング、802.1p		
認証	XAUTH/RADIUS、Active Directory、SSO、LDAP、Novell、内部ユーザデータベース、Terminal Services、Citrix		
ローカルユーザーデータベース	250	2,500	3,200

[1]PAYGは現在AWSでのみ利用可能です。
[2]Jumboフレームが無効にあるメモリ。
[3]Jumboフレームが有効にあるメモリ。Jumboフレームには追加のメモリが必要です。JumboフレームはAzureとAWSに対応しません。
[4]高可用性はVMware ESXiプラットフォーム、KVM、Azure、Microsoft Hyper-V、Nutanixで利用可能です。NSv 270では、D3v2 VMサイズを使用することによってHAをサポートします。HAはAWSではサポートされていません。AzureのHAには、3つ以上のインターフェイスをサポートしているサーバーサイズが必要です。
[5]パフォーマンス公表値は仕様に準拠しており、実際のパフォーマンスについてはハードウェアやネットワークの状態、ファイアウォール設定とアクティブ化されたサービスによって異なる場合があります。パフォーマンスおよび容量は、基盤となる仮想化インフラストラクチャによっても異なる場合があります。パフォーマンスと容量の要件を満たすために、環境内で追加テストを行うことをお勧めします。パフォーマンス測定基準は、SonicOS 7.0.1を実行するインテルXeonプロセッサー(Platinum 8268 @2.9GHz、3.9GHzターボ、37.5Mキャッシュ)とVMware vSphere 7.0を用いて確認されています。
[6]MSSPプログラムに利用できるSSL VPNクライアント数は、NSv 270では50、NSv 470では75です。SSL VPN数の増加分は、SonicOS 6.5.4.4-44v-21-723ファームウェア以降でのみご利用いただけます。
[7]VLANインターフェースは、AzureとAWSに対応しません。
テスト方法:最大パフォーマンスはRFC 2544 (ファイアウォール)に基づいています。脅威防御/ゲートウェイAV/アンチスパイウェア/IPSのスループットは、業界標準のKeysight HTTPパフォーマンステストツールを使用して測定しています。テストは、複数のポートペアでの複数のフローで行われました。脅威防御のスループットは、ゲートウェイAV、アンチスパイウェア、IPSおよびアプリケーションの制御をデフォルトのファイアウォールの設定で有効にして測定しています。VPNのスループットは、RFC 2544に準拠したAESGMAC16-256暗号を使用したパケットサイズ1418バイトのUDPトラフィックにより測定されています。仕様、機能、使用の可否については、いずれも変更される場合があります。
[8]すべてのパフォーマンスパラメータは、Dell R740をSR-IOVと共にターボブーストで使用してテストしました。
[9]プライベートクラウドではサポートされていますが、パブリッククラウドプラットフォームではサポートされていません。
[10]Nutanix AHVは、SonicOSX 7.0.0ファームウェア以降を実行しているSonicWall NSv 270/470/870でサポートされています。
[11]SonicOSX 7.0.1以降のユーザーは、クラシック/グローバルとポリシーモードとの間で選択および切り替えができます。
[12]ガバメントクラウドはBYOLでのみ使用可能です。
[13]MSSPプログラムに利用できるGVCクライアント数は、NSv 270では25、NSv 470では50です。

SonicOSX 7.0の機能概要

ファイアウォール

- ステートフルパケットインスペクション（SPI）
- Reassembly-Free Deep Packet Inspection（RFDPI）
- DDoS攻撃の防御（UDP/ICMP/SYNフラッド）
- IPv4/IPv6対応
- リモートアクセスのための生体認証
- DNSプロキシ
- REST API
- SonicWallスイッチの統合[1]
- SonicWall Wi-Fi 6 APの統合
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）
- DNSフィルタリング
- SD-WAN
  - SD-WANの拡張性
  - SD-WANのユーザビリティウィザード
- API
  - APIのフルサポート
- マルチテナント[3]
  - マルチテナントサポート
  - テナントビューとテナントごとのファームウェアサポート
- クラシック/グローバルとポリシーモードとの間で切り替え[4]

統合ポリシー

- レイヤー3からレイヤー7のルールを統合したポリシー：
  - 送信元/送信先IP/ポート/サービス
  - アプリケーション制御
  - CFS/Webボットネット/Geo-IP
  - ルールダイアグラム
  - シングルパスセキュリティサービスの適用
    – IPS/GAV/AS/Capture ATP
  - エンドポイントのプロファイルベースオブジェクト/BWM/QoS/CFS/侵入防止
- セキュリティのアクションプロファイル/DoSルール
- ルール管理：
  - クローニング
  - シャドウルール分析
  - セル内編集
  - ルールのエクスポート
  - グループ編集
- 表示管理
  - 使用済み/未使用ルール
  - アクティブ/非アクティブルール
  - セクション/カスタムグループ化
  - カスタマイズ可能なグリッド/レイアウト

TLS/SSL/SSHの復号化とインスペクション

- TLS1.3
- TLS 1.3をサポート（セキュリティを強化）
- TLS/SSL/SSH対応のディープパケットインスペクション
- オブジェクト、グループ、ホスト名の包含/除外
- SSL制御
- ゾーンまたはルールごとのきめ細かなDPI-SSL制御

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection（RTDMI）
- クラウドベースのマルチエンジン分析
- 仮想サンドボックス
- ハイパーバイザレベルの分析
- フルシステムエミュレーション
- 広範な種類のファイルの検査
- 自動および手動による送信
- リアルタイムの脅威インテリジェンスの更新
- 正体が判明するまでブロック
- Capture Client

侵入防止[2]

- シグネチャベースのスキャン
- Aruba ClearPassによるネットワークアクセス制御の統合
- シグネチャの自動更新
- 双方向インスペクション
- きめ細かなIPSルール機能
- GeoIPの適用
- 動的リストによるボットネットのフィルタリング
- 正規表現マッチング

アンチマルウェア[2]

- ストリームベースのマルウェアスキャン
- ゲートウェイアンチウイルス
- ゲートウェイアンチスパイウェア
- 双方向インスペクション
- ファイルサイズの制限なし
- クラウドのマルウェアデータベース

アプリケーションの識別[2]

- アプリケーション制御
- アプリケーションの帯域幅管理
- カスタムアプリケーションのシグネチャ作成
- データ漏洩防止
- NetFlow/IPFIXによるアプリケーションレポート機能
- 包括的なアプリケーションシグネチャのデータベース

トラフィックの可視化と分析

- ユーザーアクティビティ
- アプリケーション/帯域幅/脅威の使用状況
- クラウドベースの分析

HTTP/HTTPS Webコンテンツフィルタリング[2]

- URLフィルタリング
- プロキシの回避
- キーワードによるブロック
- レピュテーションベースのコンテンツフィルタリングサービス（CFS 5.0）
- DNSフィルタリング
- ポリシーベースのフィルタリング（除外/包含）
- HTTPヘッダーの挿入
- 帯域幅管理CFS評価カテゴリ
- アプリケーション制御可能な統合ポリシーモデル
- コンテンツフィルタリングクライアント

VPN

- セキュアSD-WAN
- VPNの自動プロビジョニング
- サイト間接続型IPSec VPN
- SSL VPNおよびIPSecクライアントリモートアクセス
- 冗長VPNゲートウェイ
- iOS、Mac OS X、Windows、Chrome、AndroidおよびKindle FireのMobile Connect
- ルートベースVPN（RIP/OSPF/BGP）

ダッシュボードの改良

- デバイス表示の改良
- 上位トラフィックとユーザー概要
- 脅威の分析情報
- 通知センター
- 強化されたパケット監視
- UIでのSSHターミナル
- 新しいデザイン/テンプレート
- 業界と世界平均の比較

ネットワーク

- PortShield[1]
- ジャンボフレーム
- Path MTU Discovery
- 強化されたログ機能
- VLANトランキング
- ポートミラーリング（NSa 2650以上）
- レイヤ2のQoS
- ポートセキュリティ
- 動的ルーティング（RIP/OSPF/BGP）
- SonicWallワイヤレスコントローラー[1]

SONICWALL

- ポリシーベースのルーティング（ToS/メトリックおよびECMP）
- NAT
- DHCPサーバー
- 帯域幅の管理
- リンクアグリゲーション[1]（スタティック、ダイナミック）
- ポート冗長性[1]
- 状態同期によるA/P高可用性
- A/Aクラスタリング[1]
- インバウンド/アウトバウンド負荷分散機能
- L2ブリッジモード[1]、ワイヤ/仮想ワイヤモード、タップモード、NATモード
- 3G/4G WANフェイルオーバー[1]
- 非対称ルーティング
- Common Access Card（CAC）のサポート
- SonicCoreXとSonicOSのコンテナ化

復号化ポリシー

- SSL/TLSトラフィックに対応する統合ポリシー

DoSポリシー

- DoS/DDoS攻撃の防御に対応する統合ポリシー

VoIP

- よりきめ細かなQoS制御
- 帯域幅の管理
- VoIPトラフィックに対するDPI
- H.323ゲートキーパーおよびSIPプロキシサポート

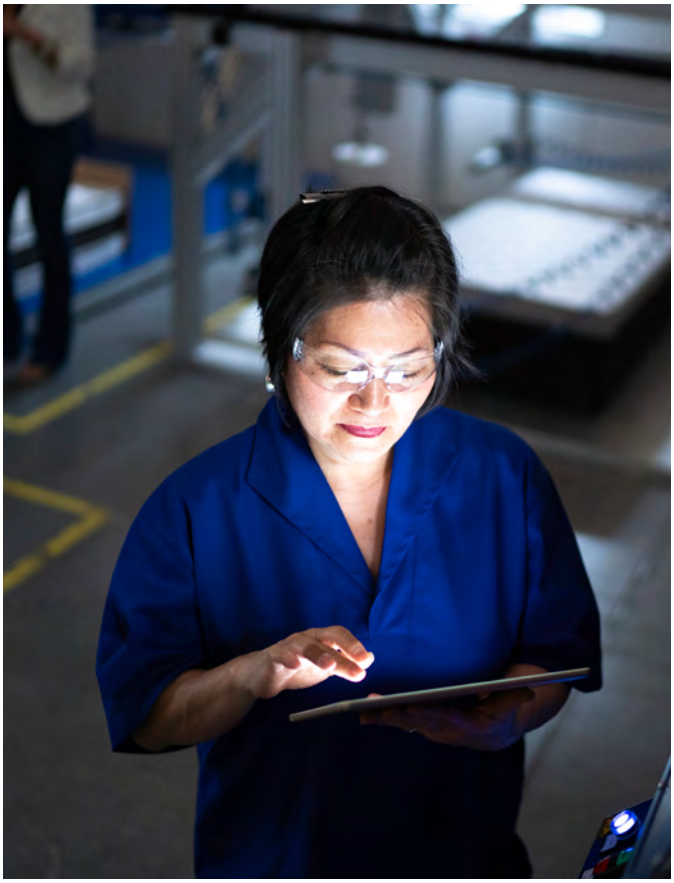
管理および監視

- Web GUI
- コマンドラインインターフェイス（CLI）
- ゼロタッチ登録とプロビジョニング
- SonicExpressモバイルアプリのサポート
- SNMPv2/v3
- Network Security Manager（NSM）による集中管理とレポート機能2
- ログ機能
- Netflow/IPFixによるエクスポート
- クラウドベースの構成バックアップ
- アプリケーションと帯域幅の可視化
- IPv4とIPv6の管理
- オフボックスレポート（Scrutinizer）
- LCD管理画面[1]
- カスケード接続のスイッチを含むDell N-SeriesおよびX-Seriesスイッチ管理[1]
- Network Security Managerレポート

ワイヤレス1

- SonicWave APクラウドおよびファイアウォール管理
- WIDS/WIPS
- 不正APの防止
- 高速ローミング（802.11k/r/v）
- 802.11sメッシュネットワーキング
- 自動チャネル選択
- RFスペクトル分析
- フロアプラン表示
- トポロジ表示
- バンドステアリング
- ビームフォーミング
- エアタイム（通信時間）の公平性
- Bluetooth Low Energy（BLE）
- MiFiエクステンダー
- ゲスト巡回割り当て
- LHMゲストポータル

[1] NSvシリーズファイアウォールではサポートされていません
[2] サブスクリプションの追加が必要です
[3] NSspファイアウォールのみで利用可能です
[4] SonicOSX 7.0.1以降で利用可能です



パートナーが提供するサービス

SonicWallソリューションの計画、導入、最適化に関して支援をお求めですか？SonicWallアドバンスド・サービス・パートナーは、お客様にワールドクラスの専門的なサービスをご提供いたします。詳細はこちら：

www.sonicwall.com/PES

SonicWall NSv 270/470/870シリーズの詳細はこちら

www.sonicwall.com/NSv

SonicWallについて

SonicWallは、安定した、拡張可能で、シームレスなサイバーセキュリティを提供することにより、誰もがリモート/モバイルで危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、中小企業をサポートします。詳しくはwww.sonicwall.comをご覧ください。

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細は当社ウェブサイトをご覧ください。
www.sonicwall.com